REMARKS

Applicants have thoroughly considered the Examiner's remarks in the April 4, 2008 Office action and have amended the application to more clearly set forth aspects of the invention. As a preliminary matter, Applicants acknowledge the Examiner's withdrawal of the October 10, 2006 Restriction Requirement (Office action, page 12) and, accordingly, the examination of claims 1-10 which were not elected for examination as a result of the Restriction Requirement.

This Amendment A amends claims 1, 4-7, 11-17, 19-22, 24, and 28. In addition, claims 2, 3, 8, 9, 18, 25, 26, 29, and 32-35 have been canceled and claims 36-41 have been added. Claims 1, 4-7, 10-17, 19-24, 28, 30, 31, and 36-41 are thus presented in the application for further examination. Reconsideration of the application as amended and in view of the following remarks is respectfully requested.

Applicants request that the Examiner review and accept the drawings as originally filed.

Claim Rejections Under 35 U.S.C. § 102(e)

Claims 1-35 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2002/0147810 to Traversat et al. (Traversat). Applicants respectfully disagree. As discussed below, Traversat fails disclose or suggest each and every feature claimed in the rejected claims.

An embodiment of the present invention is directed to a single authorization service that provides role-based access to clients for resources controlled by one or more severs/services affiliated with the authorization service. The authorization service maintains authorization data that is required by each of the affiliate services (e.g., second entity) in order to allow clients (e.g., first entity) to access the resources which are controlled by the affiliate services. Accordingly, when a client attempts to access a resource controlled by an affiliate service (e.g., a web site) and the affiliate service requests authorization data from the client, the client requests the authorization data (e.g., as a token) from the authorization service. The authorization service issues the required authorization data to the client based on a predefined role (such as non-sponsoreduser, emailuser, charteruser, admin, charteradmin, and customerservicerep) assigned to the user for which the client is requesting access. The client provides the authorization data to affiliate service. In order to ensure that that authorization data was not fraudulently obtained, the

affiliate service sends the authorization data received from the client to authorization for validation. The authorization service then validates the authorization data and notifies the affiliate service of the validation. The affiliate service accordingly provides the client with access to the requested resource.

To this end, claim 1 is directed to a method used by the authorization service to provide access to a resource for one or more users. As recited by claim 1, the method comprises:

> receiving an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users, wherein said authorization data is required by a second entity for allowing said first entity to access a resource controlled by said second entity;
>
> responsive to the received authorization request, issuing the authorization data to the first entity, wherein the first entity provides the issued authorization data to the second entity, said authorization data including an expression identifying the resource by a resource name and by at least one property associated with the resource to conditionally define access to the resource and said authorization data including validation information;
>
> receiving a validation request from the second entity to validate the issued authorization data that was provided to the second entity by the first entity; and
>
> responsive to the received validation request, validating the authorization data based on the validation information included therein.

Thus, the authorization service provides secure central management for resources in distributed services so that each of the services need not maintain user authentication data and perform user authentication. Additionally, by providing role-based access control of resources, the present invention simplifies access control management across resources that are associated with multiple services. Thus, the present invention allows administrators to specify access control in terms of the roles within an organization and may be used in a federated environment.

In contrast, Traversat merely discloses protocols for implementing in a peer-to-peer environment for allowing the peer nodes to discover each other, communicate with each other, and cooperate with each other to form peer groups and share network resources. Traversat mentions that "[e]ach peer group may include one or more peers that may serve as a certificate

authority in the group." (Traversat, paragraph [0441]). "The process of joining a peer group may include obtaining a credential that is used to become a group member . . . or obtaining a "form" listing the set of requirements asked of all group members." (Traversat, paragraph [0363]). An agreement (e.g., social contract) between the peers in the peer group defines how a peer may access data once the peer has joined the peer group. For example, the peer group may be configured such that a "member of a group is automatically granted access to all data offered by another member for sharing, whereas non-members cannot access such data." (Traversat, paragraph [0436]). Alternatively, "certificates and/or public keys may be exchanged without the participation of a strict certificate authority; i.e. the members may exchange certificates based upon their trust in each other. (Traversat, paragraph [0441]).

In other words, Traversat merely discloses a peer authority for assessing a level of trust of a particular peer in or attempting to join a peer group. The individual peers in the peer group can then determine whether to provide the particular peer with access to data based on the assessed level of trust. For example, an individual peer in the peer group may allow the particular peer to assume a particular role if the peer authority has indicated that the particular peer has a trust level which the individual peer requires for the role.

This is completely different from the method recited by claim 1. Traversat fails to teach that the peer authority authorizes the particular peer for access to specific resources associated with a role assigned to the peer. Accordingly, Traversat fails to teach aspects of claim 1, including, "receiving an authorization request from a first entity to issue authorization data for the one or more users ***based on roles associated with the users***, wherein said authorization data is required by a second entity for allowing said first entity to access a resource controlled by said second entity" and "***said authorization data including an expression identifying the resource*** by a resource name and by at least one property associated with the resource to conditionally define access to the resource." Thus, Traversat fails to provide central management for resources in distributed services so that each of the services (peers) need not maintain the credentials (e.g., level of trust) needed for accessing particular resources.

Even if Traversat taught that the peer authority issued authorization data for a specific resource based on the role of the particular peer, Traversat fails to teach that the peer authority validates the issued authorization data so that the particular peer can access the identified resource. In fact, Traversat teaches away from the present invention by teach that "the members

may exchange certificates based upon their trust in each other" (Traversat, paragraph [0441]). Thus, Traversat fails to teach aspects of claim 1, including "receiving a validation request from the second entity to validate the issued authorization data that was provided to the second entity by the first entity" and "responsive to the received validation request, ***validating the authorization data based on the validation information included therein***." (emphasis added). Since Traversat fails to provide the validation for the authorization data, Traversat fails to provide an authorization service which minimizes vulnerability to fraudulent attacks (e.g., replay attacks).

As such, Traversat fails to disclose or suggest each and every limitation of amended claim 1. Applicants submit that the rejection of amended claim 1 under 35 U.S.C. §102 should be withdrawn.

Amended independent claims 11, 24, and 28 include limitations similar to those included in amended claim 1. As such, Applicants submit that Traversat fails to disclose or suggest each and every limitation of amended independent claims 11, 24, and 28. Amended claims 11, 24, and 28 are allowable for at least the same reasons that amended claim 1 is allowable. Additionally, the claims that depend from amended independent claims 11, 24, and 28 are allowable for at least the reasons that the independent claims from which they depend are allowable.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. Applicants thus respectfully submit that claims 1, 4-7, 10-17, 19-24, 28, 30, 31, and 36-41 as presented are in condition for allowance and respectfully request favorable reconsideration of this application.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and

encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Robert M. Bain/

Robert M. Bain, Reg. No. 36,736
SENNIGER POWERS LLP
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

RMB/NAS/eaw